LAMPS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 25 January 2023

M. Richardson, Ed.
Sandelman Software Works
O. Friel
Cisco
D. von Oheimb
Siemens
D. Harkins
The Industrial Lounge

24 July 2022

# Clarification of RFC7030 CSR Attributes definition
# draft-richardson-lamps-rfc7030-csrattrs-04

## Abstract

The Enrollment over Secure Transport (EST, RFC7030) is ambiguous in its specification of the CSR Attributes Response. This has resulted in implementation challenges and implementor confusion.

This document updates RFC7030 (EST) and clarifies how the CSR Attributes Response can be used by an EST server to specify both CSR attribute OIDs and also CSR attribute values that the server expects the client to include in subsequent CSR request.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 January 2023.

## Copyright Notice

Table of Contents



## 1. Introduction

Enrollment over Secure Transport [RFC7030] (EST) has been used in a wide variety of applications. In particular, [RFC8994] and [RFC8995] describe a way to use it in order to build out an autonomic control plane (ACP) [RFC8368].

The ACP requires that each node be given a very specific SubjectAltName. In the ACP specification, the solution was for the EST server to use section 2.6 of [RFC7030] to convey to the EST client the actual SubjectAltName that will end up in its certificate.

As a result of some implementation challenges, it came to light that this particular way of using the CSR attributes was not universally agreed upon, and it was suggested that it went contrary to section 2.6.

Section 2.6 says that the CSR attributes "provide additional descriptive information that the EST server cannot access itself".

After significant discussion, it has been determined that Section 4.5 of [RFC7030] specification is sufficiently difficult to read that clarification is needed.

This document motivates the different use cases, and provides additional worked out examples.

This document also updates section 4.5 to include revised ASN.1 that covers all uses and is backward compatible with the existing use.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. CSR Attributes Handling

### 3.1. Current EST CSR Attributes Specification

The ASN.1 for CSR Attributes as defined in EST section 4.5.2 is:

```
CsrAttrs ::= SEQUENCE SIZE (0..MAX) OF AttrOrOID

AttrOrOID ::= CHOICE (oid OBJECT IDENTIFIER, attribute Attribute }

Attribute { ATTRIBUTE:IOSet } ::= SEQUENCE {
     type   ATTRIBUTE.&id({IOSet}),
     values SET SIZE(1..MAX) OF ATTRIBUTE.&Type({IOSet}{@type}) }
```

### 3.2. Revised/Simplified EST CSR Attributes Specification

(XXX: This isn’t really simpler, is it?)

```
CsrAttrs ::= SEQUENCE SIZE (0..MAX) OF AttrOrOID

AttrOrOID ::= CHOICE (oid OBJECT IDENTIFIER,
                      attribute Attribute }

Attribute { ATTRIBUTE:IOSet } ::= SEQUENCE {
     extType  ATTRIBUTE.&id({IOSet}),
     extAttr  SET SIZE(1..MAX) OF ATTRIBUTE.&Type({IOSet}{@type})
}
```

A key part that was unclear is that extAttr above could be an entire Extension, as per Section 4.2 of [RFC5280]. This structure naturally includes both the extention ID, a critical bit, and the extension value.

The extType for such an extension would be "ExtensionRequest" (extReq), which is OID 1.2.840.113549.1.9.14.

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING
                 -- contains the DER encoding of an ASN.1 value
                 -- corresponding to the extension type identified
                 -- by extnID
     }
```

With this understand, the needs of [RFC8994] and [RFC8995] are satisfied, however with a change to the bits on the wire.

# 4. Co-existence with existing implementations

# 5. Examples

## 5.1. RFC8994/ACP subjectAltName with specific otherName included

This is a dump in "dumpasn1" format of a CSR Attributes object which a specific otherName included.

```
  0  90: SEQUENCE {
  2  88:   SEQUENCE {
  4   9:     OBJECT IDENTIFIER extensionRequest (1 2 840 113549 1 9 14)
 15  75:     SET {
 17  73:       SEQUENCE {
 19   3:         OBJECT IDENTIFIER subjectAltName (2 5 29 17)
 24   3:         [0] {
 26   1:           BOOLEAN TRUE
       :           }
 29  61:         SEQUENCE {
 31  59:           [0] {
 33  57:             UTF8String
       :               'rfc8994+fd739fc23c34401122334455000000000+@acp.ex'
       :               'ample.com'
       :             }
       :           }
       :         }
       :       }
       :     }
       :   }
```

## 5.2. EST server requires public keys of a specific size

TBD

## 5.3. EST server requires a public key of a specific algorithm/curve

TBD

## 5.4. EST server requires a specific extension to be present

TBD

# 6. Security Considerations

All security considertions from EST [RFC7030] section 6 are applicable.

## 6.1. Identity and Privacy Considerations

An EST server may use this mechanism to instruct the EST client about the identities it should include in the CSR it sends as part of enrollment. The client may only be aware of its IDevID Subject, which includes a manufacturer serial number. The EST server can use this mechanism to tell the client to include a specific fully qualified domain name in the CSR in order to complete domain ownership proofs required by the CA. Additionally, the EST server may deem the manufacturer serial number in an IDevID as personally

identifiable information, and may want to specify a new random opaque identifier that the pledge should use in its CSR. This may be desirable if the CA and EST server have different operators.

## 7. IANA Considerations

No requests are made to IANA.

## 8. Acknowledgements

TODO

## 9. Changelog

## 10. References

### 10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <https://www.rfc-editor.org/info/rfc8994>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

### 10.2. Informative References

[RFC8368] Eckert, T., Ed. and M. Behringer, "Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)", RFC 8368, DOI 10.17487/RFC8368, May 2018, <https://www.rfc-editor.org/info/rfc8368>.

## Authors' Addresses

Michael Richardson (editor)
Sandelman Software Works
Email: mcr+ietf@sandelman.ca

Owen Friel
Cisco
Email: ofriel@cisco.com

Dr. David von Oheimb
Siemens
Email: dev@ddvo.net

Dan Harkins
The Industrial Lounge
Email: dharkins@lounge.org